(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 April 2003 (10.04.2003)

PCT

(10) International Publication Number
WO 03/030474 A2

(51) International Patent Classification[7]: H04L 12/58, 29/06, 29/12

(21) International Application Number: PCT/IE02/00139

(22) International Filing Date:
30 September 2002 (30.09.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/325,204 28 September 2001 (28.09.2001) US
01 650 118.1 8 October 2001 (08.10.2001) EP

(71) Applicant *(for all designated States except US)*: **MARKPORT LIMITED** [IE/IE]; Custom House Plaza 5, Harbourmaster Place, Dublin 1 (IE).

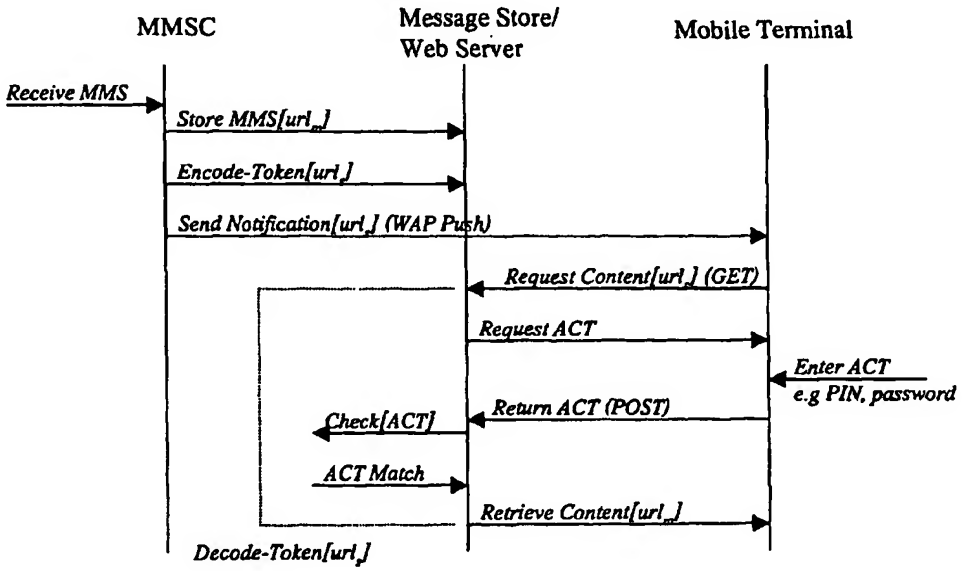
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **JONES, Frederick, James** [IE/IE]; Rose Cottage, Lower Road, Shankill (IE). **O'SULLIVAN, Fergal** [IE/IE]; 13 Priory Court, St. Raphael's Manor, Celbridge, County Kildare (IE). **MURTAGH, John** [IE/IE]; 25 Finsbury House, Pembroke Road, Dublin 4 (IE). **JOHNSON, Joseph** [IE/IE]; 43 Holmwood, Brennanstown Road, Dublin 18 (IE). **CORRIGAN, Louis** [IE/IE]; Jordanstown, Enfield, County Meath (IE). **MCGEE, Brendan** [IE/IE]; Oakdene, 55 South Avenue, Mount Merrion (IE).

(74) Agents: **O'BRIEN, John, A.** et al.; John A. O'Brien & Associates, Third Floor, Duncairn House, 14 Carysfort Avenue, Blackrock, Dublin (IE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[Continued on next page]

(54) Title: MMSC ACCESS CONTROL



Token Handling - Subscriber Challenge

(57) Abstract: An MMSC generates an encoded token based on a message-locator (or part-locator) and the recipient's subscription identification. The token is inserted in the message-locator (or part-locator) field of a notification sent to the recipient. When a MMS message request is received, the MMS decodes the message-locator (or part-locator) field to authenticate the subscriber and the locator. This authentication effectively allows access from a substitute URL location included in the notification to a real URL location for the content.

WO 03/030474 A2

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

"MMSC Access Control"

INTRODUCTION

Field of the Invention

The invention relates to communication of rich messages having content in a mobile network environment. An example is routing of multi-media messages in which a multi-media service centre (MMSC) is used. Another example is in WAP or I-Mode in which a notification is pushed to a subscriber and the subscriber then uses a browser to pull the notified content.

Prior Art Discussion

In normal operating mode, an MMSC receives a MIME encoded Multimedia Message or E-mail message as defined by the 3GPP, WAP Forum and IETF. This message may contain multimedia elements (e.g. text, audio, video etc.). This message is stored temporarily in an MMSC message store and a notification is sent to one or more mobile device(s) indicating the message characteristics (e.g. size etc.) and a unique *message-locator*, which can be used to retrieve the message. The device/subscriber then retrieves the MMS message using the *message-locator* received in the notification.

The multimedia parts of the message may contain the actual multimedia content, or may contain a further *part-locator* which can be used to retrieve the multimedia content. This is typically used in applications where the multimedia content (voice / video) is too large to be stored on the device and is instead streamed from a server in the network.

United States Patent Specification No. US6246871B (Nokia) describes a method of messaging in which a notification includes a temporary access code for the stored message. Such a notification is sent to multiple recipients, who can then

access the message using the temporary access code. PCT Patent Specification No. WO98/58332 (Ericsson) describes a messaging method in which a notification is sent to an intended recipient, the notification having a security key.

These messaging methods provide a degree of security for the recipient by verifying the identity of the sender and limiting access to message content. However, the security is at the level of the sender or message only, and there is little control or knowledge of who is accessing the message content. This is a problem in any situation where a user wishes to notify a recipient of the location of a message or other content, and ensure that only the intended recipient will be allowed to access the content. This situation arises particularly in the context of a multi-media message delivery by an MMSC.

SUMMARY OF THE INVENTION

According to the invention, there is provided a method of communication of a rich message from a sender device to a recipient device, the method comprising the steps of:-

the sender device transmitting the message to a messaging system;

the messaging system storing content of the message, and transmitting a notification of the message to the recipient device, and

the recipient device requesting the content by accessing the messaging system and retrieving the content,

characterised in that,

the messaging system performs recipient authentication before allowing the recipient device to have access to the content.

In one embodiment, the messaging system is an MMSC and the message is a multimedia message.

In another embodiment, the messaging system includes in the notification an address of a substitute location for the content, said substitute location being different from a real location at which the content is stored, and the authentication step controls access to the real location.

In a further embodiment, the locations are URLs.

In one embodiment, said notification includes a code generated by an encode function of the messaging system, and the authentication step is performed by a decode function.

In another embodiment, the encode function generates the code using recipient data.

In a further embodiment, the decode function performs authentication by decoding the recipient data and comparing it with recipient data received in the content request.

In one embodiment, the recipient data includes a recipient subscriber identifier.

In another embodiment, the recipient subscriber identifier is an MSISDN.

In a further embodiment, the encode function uses the real location address to generate the code, and the decode function determines the real location address by decoding.

In one embodiment, the code is included in a field of the substitute location address in the notification.

In another embodiment, the encode function uses a secret key to generate the code, and the decode function uses said key to decode the code.

In a further embodiment, the secret key is randomly generated for each message.

In one embodiment, the encode function uses a recipient's PKI public key to generate the code and the decode function requests the recipient device to decode the code using its private key and subsequently verifies the recipient device decoding.

In another embodiment, the messaging system comprises the decode function.

In a further embodiment, the recipient device comprises the decode function.

According to another aspect, the invention provides a communication device comprising means for performing recipient device steps of a method as defined above.

The recipient device may, for example, be a multimedia-enabled mobile device.

According to another aspect, the invention provides a messaging system comprising means for performing messaging system steps of a method as defined above.

The messaging system may, for example, be an MMSC

In this specification, it is an assumption that an authentication of the subscriber access is performed at initial access to the underlying wireless data network (e.g. GPRS, 2G etc.), and the resulting authenticated subscriber identity information (e.g. IMSI, MSisdn, MIN etc.) is made available to the MMSC. This information, if available, can be used as part of an access control function in an

implementation of the invention, although alternative implementations may realise access control functions that do not rely on such information.

DETAILED DESCRIPTION OF THE INVENTION

Brief Description of the Drawings

The invention will be more clearly understood from the following description of some embodiments thereof, given by way of example only with reference to the accompanying drawings in which Figs. 1 to 3 are message flow diagrams of messaging methods of the invention.

Description of the Embodiments

In the invention a message is communicated by:

(a) a messaging system (such as an MMSC) transmitting a notification to a recipient, the notification indicating where message content can be retrieved, and

(b) the recipient device (typically a mobile device) accessing the server storing the message content but importantly, only being allowed access to the content after authentication of the recipient.

Thus, the invention provides security at the level of the recipient. Heretofore, control of access by recipients has been achieved by transmitting the notification only to the described recipient(s). However if the notification is wrongly routed or finds its way to a wrong recipient, or if the message location is accessed by an unintended recipient, there is inadequate control over who accesses the content despite message or sender-level security being imposed.

In one embodiment, the messaging system and the content server is an MMSC. The MMSC contains a *token-encode* function for generation of a *token* using the following:

- Recipient's subscription identification
- Actual MMSC *message-locator* or *part-locator*
- Optionally, a secret key
- Optionally, this secret key could be generated randomly for each message

The MMSC contains a *token-decode* function for extraction of the recipient subscriber identification and the actual *message-locator* or *part-locator* using the following:

- The *token*
- Optionally, the requester's subscription identification
- If used in generation of the *token*, the secret key

The design of the *token-encode* and *token-decode* functions are such that it will not be feasible in practice for a 3rd party to generate an alternative *token* such that the *token-decode* function will produce the original *message-locator* or *message-part* but with the recipient subscriber identification of the 3rd party, rather than the intended recipient.

Token Handling for *message-locator*

The MMSC receives the multimedia message from a content supplier indicating a need for *token* generation. The message is stored in the MMSC server. A *token* is generated using the *token-encode* function and is incorporated into a field used as a substitute *message-locator*. The substitute message-locator addresses a placeholder location (URL), the content being stored in a different, "real" URL location. The MMSC then notifies the recipient of the pending message using the substitute *message-locator*.

At some later time, the user ("the requester", which should be the recipient), requests the message from the MMSC using the substitute *message-locator*. The MMSC applies the *token-decode* function to extract the recipient subscription identification and the actual *message-locator*. The MMSC then compares the recipient subscription identification with the subscription identification of the requester. If they match, and the *message-locator* identifies a valid message, the message is transmitted to the requester. Thus, the decode function effectively performs recipient authentication for controlling access from the placeholder location to the real location.

A single message may be intended for several recipients. In this case separate tokens and *message-identifiers* are generated for each recipient and are validated individually. The important point is that the security is at the recipient level.

Token Handling for *part-locator*

The MMSC receives the Multimedia Message from a content supplier indicating a need for *token* generation. The message is stored in the MMSC server. For each multimedia part which contains a *part-locator* rather than the actual multimedia content, a *token* is generated using the *token-encode* function and is incorporated into the message as a substitute *part-locator*.

When the message has been received, the user ("the requester", which should be the recipient) requests (e.g. from a streaming server) the content referenced by each *part-locator*. The MMSC applies the *token-decode* function to extract the recipient subscription identification and each actual *part-locator*. The MMSC then compares the recipient subscription identification with the subscription identification of the requester. If they match, and the *part-locator* identifies a valid multimedia object, the multimedia content is transmitted (e.g. streamed) to the requester.

Further examples of implementation of the invention, in which a number of alternative *token-encode* and *token-decode* mechanisms are described, are described below with reference to Figs. 1 to 3. For these examples, an implementation of the MMSC message store based on standard Web Server capabilities is assumed, i.e. message locators are implemented by URL's, and message content is downloaded using the HTTP protocol.

Token Handling to invoke a Subscriber Challenge (Fig. 1)

The MMSC receives a multimedia message from a content supplier indicating a need for *token* generation. The message is stored in the MMSC server under a dynamically generated URL - url_m. A *token* is generated using the *token-encode* function and is incorporated into a field of a substitute *message-locator*, i.e. a substitute URL – url_s. The MMSC then notifies the recipient of the pending message using the substitute *message-locator*, url_s.

The *token-encode* function used in this implementation accesses a secure database to retrieve an access control token (ACT) that is uniquely associated with the recipient, e.g. this could be a secret PIN number or password assigned to or selected by the subscriber. The access control token is encoded, along with the actual message URL url_m, using a secret key known only to the MMSC and incorporated into a field of the substitute URL url_s.

At some later time, the user ("the requester", which should be the recipient), requests the message from the MMSC by invoking a HTTP GET method on the substitute URL url_s. The MMSC applies the *token-decode* function, which may be invoked as a CGI script or Java servlet associated with the substitute URL url_s..

The *token-decode* function extracts the access control token and the actual message URL url_m using the secret key. The MMSC responds to the request by generating a challenge to the requester to enter their access control token (ACT, e.g. PIN or password). The requester returns the requested information using a HTTP POST

method. For added security, this exchange could use HTTPS to ensure the access control token was not exchanged in plain-text. The *token-decode* function now compares the received access control token with the access control token that was decoded from the substitute URL url_s. If the access control tokens match, the requester is authenticated and the message content stored under the actual URL url_m, can be returned to the requestor.

Token Handling with Comparison to Subscriber's Network Identity (Fig. 2)

The MMSC receives the multimedia message from a content supplier indicating a need for *token* generation. The message is stored in the MMSC server under a dynamically generated URL - url_m. A *token* is generated using the *token-encode* function and is incorporated into a field of a substitute *message-locator*, i.e. a substitute URL – url_s. The MMSC then notifies the recipient of the pending message using the substitute *message-locator*, url_s.

The *token-encode* function used in this implementation retrieves the recipient's network identity from the destination address of the message, e.g. this could be an MSISDN, MIN or similar identifier. The subscriber identity is encoded, along with the actual message URL url_m, using a secret key known only to the MMSC and incorporated into a field of the substitute URL url_s.

At some later time, the user ("the requester", which should be the recipient), requests the message from the MMSC by invoking a HTTP GET method on the substitute URL url_s. The MMSC applies the *token-decode* function, which may be invoked as a CGI script or Java servlet associated with the substitute URL url_s..

The *token-decode* function extracts the subscriber identifier and the actual message URL url_m using the secret key. The *token-decode* function now compares the subscriber identifier provided by the network with the subscriber identifier that was decoded from the substitute URL url_s. If the subscriber identifiers match, the

requester is authenticated and the message content stored under the actual URL url_m, can be returned to the requestor.

Token Handling with Public Key Cryptography (Fig. 3)

The MMSC receives the Multimedia Message from a content supplier indicating a need for *token* generation. The message is stored in the MMSC server under a dynamically generated URL - url_m. A *token* is generated using the *token-encode* function and is incorporated into a field of a substitute *message-locator*, i.e. a substitute URL – url_s. The MMSC then notifies the recipient of the pending message using the substitute *message-locator*, url_s.

The *token-encode* function first generates a unique access control token using a suitable random function. It then retrieves the recipient's PKI certificate and uses the recipient's public key to encode the access control token - act_u. The access control token is also encoded using a secret key known only to the MMSC – act_m. The actual message URL url_m is also encoded using a secret key known only to the MMSC and all values are incorporated into a field of the substitute URL url_s.

At some later time, the user ("the requester", which should be the recipient), requests the message from the MMSC by invoking a HTTP GET method on the substitute URL url_s. The MMSC applies the *token-decode* function, which may be invoked as a CGI script or Java servlet associated with the substitute URL url_s..

The *token-decode* function extracts act_u. It also decodes act_m and the actual message URL url_m using the secret key. The MMSC responds to the request by sending the act_u to the requester and asking them to return the decrypted access control token. The requester's mobile terminal decrypts the act_u using the subscriber's private key (stored in a secure fashion on the mobile terminal). The decrypted access control token is returned. As the access control token is a randomly generated, single use token, it is not necessary to use HTTPS for the exchange. The *token-decode* function now compares the decrypted access control token received from the

subscriber with the decrypted act_m. If the access control tokens match, the requester is authenticated and the message content stored under the actual URL url_m, can be returned to the requestor.

It will be appreciated that the invention provides a very effective mechanism for sending messages with content to only intended recipients. This is very advantageous for ensuring privacy and confidentiality in a range of messaging scenarios, such as communication of sensitive business information.

While the invention has been described in the context of mobile networks, it is envisaged that the recipient may use a land-line telephone or other communication device to pull down the content. This may occur, for example, if the functionalities of mobile and fixed phones converge in later years. In an alternative implementation of the invention, the *token-decode* function might be contained in the recipient device. Also, the embodiments described use subscriber data (MSISDN or MIN) to encode the notification. Such data is associated specifically with the user and not necessarily the user's device. For example, the MSISDN may be stored in the user's SIM card. The encode function may alternatively use a device identifier such as an IMEI or GSM network.

The invention is not limited to the embodiments described but may be varied in construction and detail.

Claims

1. A method of communication of a rich message from a sender device to a recipient device, the method comprising the steps of:-

the sender device transmitting the message to a messaging system;

the messaging system storing content of the message, and transmitting a notification of the message to the recipient device, and

the recipient device requesting the content by accessing the messaging system and retrieving the content,

characterised in that,

the messaging system performs recipient authentication before allowing the recipient device to have access to the content.

2. A method as claimed in claim 1, wherein the messaging system is an MMSC and the message is a multimedia message.

3. A method as claimed in claims 1 or 2, wherein the messaging system includes in the notification an address of a substitute location for the content, said substitute location being different from a real location at which the content is stored, and the authentication step controls access to the real location.

4. A method as claimed in claim 3, wherein the locations are URLs.

5. A method as claimed in any preceding claim, wherein said notification includes a code generated by an encode function of the messaging system, and the authentication step is performed by a decode function.

6. A method as claimed in claim 5, wherein the encode function generates the code using recipient data.

7. A method as claimed in claim 6, wherein the decode function performs authentication by decoding the recipient data and comparing it with recipient data received in the content request.

8. A method as claimed in claim 7, wherein the recipient data includes a recipient subscriber identifier.

9. A method as claimed in claim 8, wherein the recipient subscriber identifier is an MSISDN.

10. A method as claimed in any of claims 5 to 9, when dependent on claims 3 or 4, wherein the encode function uses the real location address to generate the code, and the decode function determines the real location address by decoding.

11. A method as claimed in claim 10, wherein the code is included in a field of the substitute location address in the notification.

12. A method as claimed in any of claims 5 to 11, wherein the encode function uses a secret key to generate the code, and the decode function uses said key to decode the code.

13. A method as claimed in claim 12, wherein the secret key is randomly generated for each message.

14. A method as claimed in any of claims 5 to 13, wherein the encode function uses a recipient's PKI public key to generate the code and the decode function requests the recipient device to decode the code using its private key and subsequently verifies the recipient device decoding.

15. A method as claimed in any of claims 5 to 14, wherein the messaging system comprises the decode function.

16. A method as claimed in any of claims 5 to 14, wherein the recipient device comprises the decode function.

17. A messaging system comprising means for performing messaging system steps of a method as claimed in any preceding claim.

18. A messaging system as claimed in claim 17, wherein the messaging system is an MMSC.

19. A communication device comprising means for performing recipient device steps of a method as claimed in any preceding claim.

20. A communication device as claimed in claim 19, wherein the communication device is a multimedia-enabled mobile device.

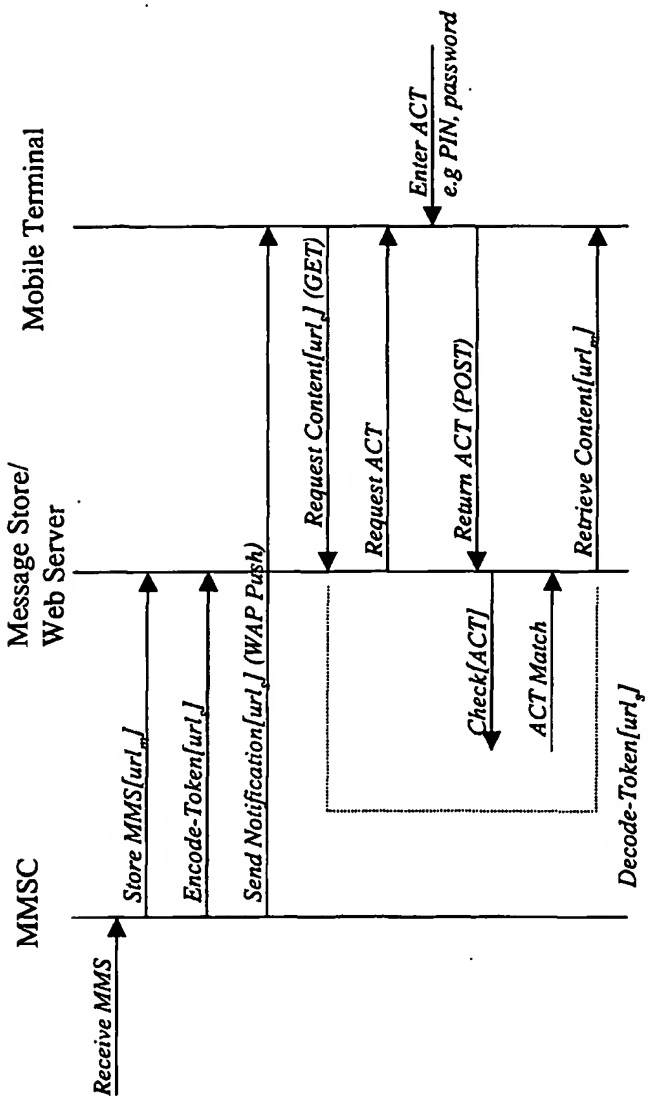


Fig. 1: Token Handling - Subscriber Challenge

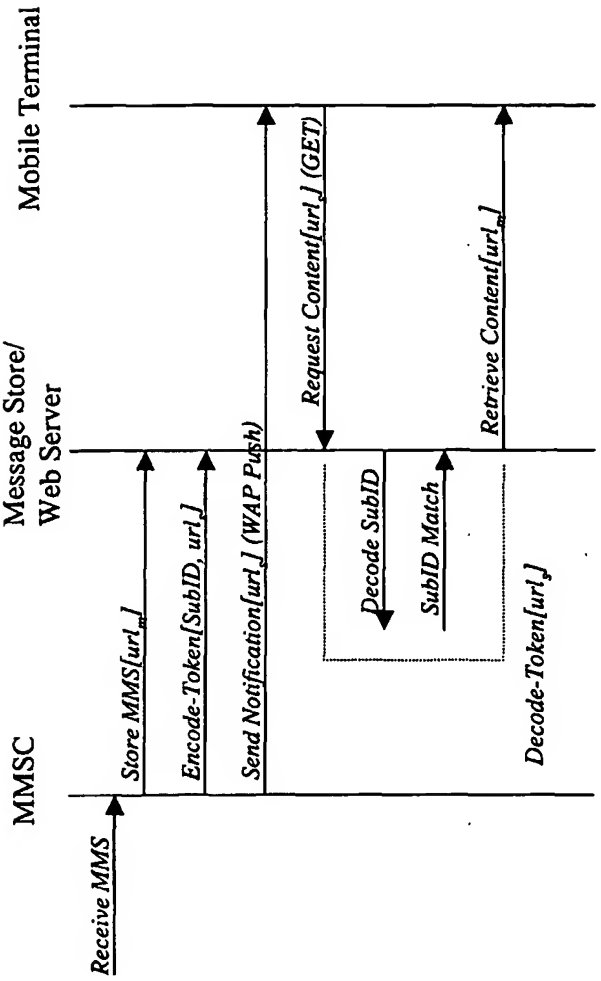


Fig. 2: Token Handling - Subscriber Network Identity

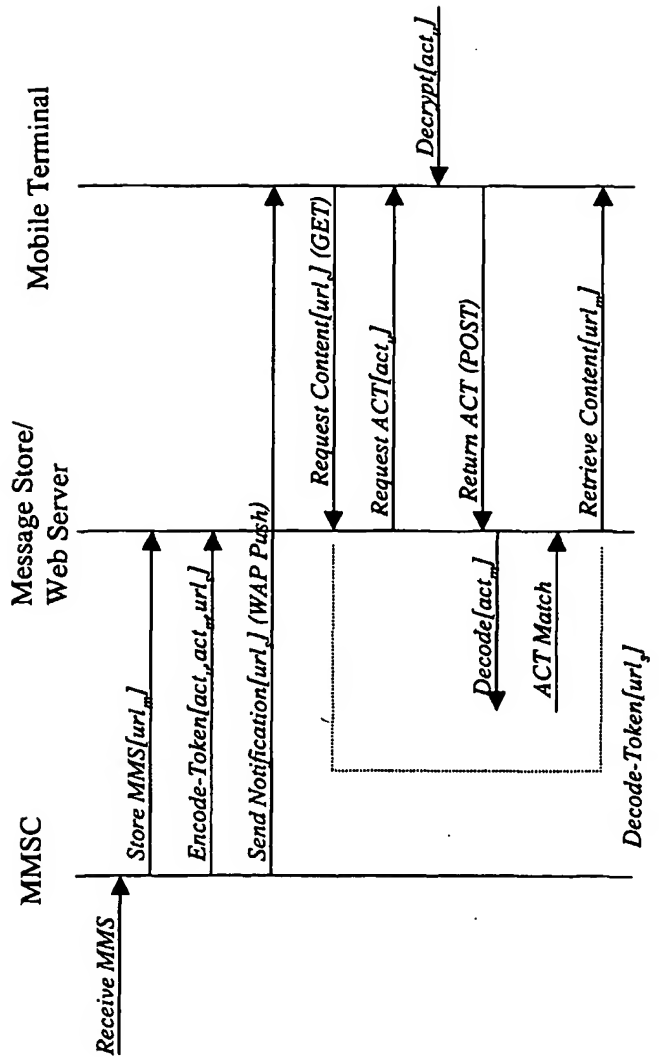


Fig. 3: Token Handling - Public Key Cryptography